УДК 3302.34 https://doi.org/10.31713/ve2201835

Міщук Г. Ю., д.е.н., професор (Національний університет водного господарства та природокористування, м. Рівне),
Комар С. О., студентка (Національний університет водного господарства та природокористування, м. Рівне)

КІБЕРЗЛОЧИННІСТЬ ЯК НАСЛІДОК РОЗВИТКУ ІТ-РИНКУ: ОЦІНКА ВИКЛИКІВ ДЛЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

Проаналізовано динаміку кіберзлочинів в Україні впродовж 2015–2018 років. Встановлено, що кіберзлочинність як один з негативних наслідків розвитку ІТ-ринку є тим видом злочинів, протидія яким поки що не має достатнього розвитку в Україні. Маючи обмеження також у статистичних даних щодо її наслідків для фінансово-економічної безпеки, використано зарубіжний досвід для характеристики втрат підприємств та значимості в числі глобальних ризиків людства. Запропоновано застосування прогресивного світового досвіду для посилення кібербезпеки в Україні. Основними з них визначено дії щодо посилення обізнаності користувачів щодо кіберзагроз та поведінки у таких ситуаціях, розвиток ринку кіберстрахування, а також посилення державного контролю національного кіберпростору.
Ключові слова: **ІТ-ринок, кібербезпека, кіберзлочинність, фінансово-економічні наслідки.**

Вступ. Розвиток ІТ-ринку дає сьогодні найбільше можливостей швидкого економічного зростання, відтак увага до процесів його розвитку характерна для країн з різним рівнем конкурентоспроможності. Разом з тим, при справді суттєвих економічних перевагах, негативним наслідком швидкого прогресу ІТ-технологій та стрімкого зростання кількості фахівців у цій галузі є так само швидке поширення кібернебезпек, впливу яких зазнають уже не лише окремі компанії та фізичні особи – іноді під загрозою опиняється робота об'єктів інфраструктури, критично важливих для забезпечення національної безпеки. Відтак, кіберзлочинність та методи її попередження або хоча б компенсації наслідків є сьогодні актуальною проблемою, прогрес у розв'язанні якої дозволить зменшити частину важливих для України небезпек, в тому числі фінансово-економічних.

Аналіз останніх досліджень. Кіберзагрози та кіберзлочинність є визнаною проблемою всього людства, про що свідчить наявність

цього виду ризиків у числі глобальних ризиків, що щорічно моніторяться Всесвітнім економічним форумом (далі ВЕФ) [1]. Визнання вагомості кіберзагроз, їх швидкого поширення і в Україні зумовило потребу прийняття відповідного Закону України [2], де чітко закріплено поняття кіберзагроз, кіберпростору, кіберзлочинності та визначені засади налагодження системи безпечного використання даних в інформаційних мережах. Зростання кількості та наслідків кібератак як одного з видів кіберзлочинів зумовлює значну увагу до цього об'єкта досліджень не лише фахівців-практиків, але й наукового загалу – у цьому контексті на сьогодні проводяться дослідження не лише з точки зору кібербезпеки в аспекті її технічного забезпечення, але й з боку економічних засад аналізу відповідних небезпек [3; 4; 5].

Постановка завдання. Враховуючи існуючі тенденції розвитку IT-ринку та зростаючу роль кіберзагроз у всіх сферах суспільних відносин, в тому числі економічних, ціллю нашого дослідження є оцінка тенденцій та наслідків кіберзлочинності в Україні в контексті забезпечення фінансово-економічної безпеки.

Наукові результати. У світі вагомість безпеки користування даними оцінена досить високо, зокрема, у 2007 році кіберризики вперше з'явились у переліку не лише топ-10, але й топ-5 глобальних ризиків людства на найближчий рік. Вони, щоправда, мали не таку вагомість, як інші, наприклад, глобальне потепління чи продовольча безпека, але вперше названі як характерні для всієї планети ризики, а за ймовірністю настання взагалі оцінені як найбільш можливі, порівняно з іншими. Перша позиція в рейтингу була зумовлена прогнозами високої ймовірності порушень в роботі критичної інфраструктури за рахунок кібервтручань. Наступного разу кіберризики у вигляді можливих кібератак з'явились у топ-5 у 2012 році [1]. Показовим є те, що вже з 2014 року кіберризики стали постійно актуальними для людства: вони хоч і з різною вагомістю, але займають стабільно високі позиції в рейтингу десяти найбільш значимих глобальних ризиків (табл. 1).

Таблиця 1

Наявність кіберризиків у рейтингу глобальних ризиків людства, що визначаються Всесвітнім економічним форумом
(складено авторами за даними [1])

Місце в рейтингу	Роки			
	2017	2016	2015	2014
За ймовірністю	**5** (шахрайство чи крадіжка даних) **6** (кібератаки)	**9** (шахрайство чи крадіжка даних)	**9** (шахрайство чи крадіжка даних) **10** (кібератаки)	**5** (кібератаки)

продовження табл. 1

За впливом	X	X	**7** (порушення роботи критичної інфраструктури)	**5** (порушення роботи критичної інфраструктури)

* X – не входить в топ-10

Як бачимо, в більш ранніх періодах кіберризики не мали настільки негативного характеру – пошкодження інфраструктури, в т.ч. і критичної, могли бути наслідком не обов'язково спланованого хакерського нападу, а поодиноких впливів або й об'єктивних збоїв роботи інформаційних систем. Але, починаючи з 2012 року світ зіштовхнувся з ризиками масових кібератак, а вже з 2015 року одним з найбільш імовірних для людства ризиків стали шахрайство та крадіжка даних з використанням інформаційних мереж.

Важливим кроком щодо формування кібербезпеки шляхом протидії кіберзлочинності в Україні є ратифікація у 2006 році основного міжнародного документа у цій сфері – Конвенції Ради Європи про кіберзлочинність [6]. Вона дозволяє використовувати потенціал міжнародного співробітництва для захисту кіберпростору спільними діями держав, що також ратифікували конвенцію.

З огляду на класифікацію кіберзлочинів, викладених у конвенції, можна вважати, що сьогодні найбільш поширеними напрямками втручання у кіберпростір держав та окремих фізичних та юридичних осіб є дії, що віднесені до перших двох груп кіберзлочинів (вони у конвенції викладені найбільш детально). Зокрема, до першої групи належать злочини, спрямовані на порушення конфіденційності та цілісності комп'ютерних даних та систем [6, ст. 2-6], а до другої – підробка та шахрайство з використання комп'ютерних технологій [6, ст. 7, 8]. Третю групу злочинів складають злочини, пов'язані з контентом (змістом) даних, зокрема дитяча порнографія, а четверту – порушення авторського права і суміжних прав [6, ст. 9, 10].

Таким чином, бачимо, що окремі напрями порушення безпеки кіберпростору виникли лише як реакція на нові можливості поширення протизаконної інформації. Більшого розвитку набуло створення нових видів шкідливого інформаційного контенту та нових інформаційних засобів використання чужих даних, спрямовані на отримання незаконної економічної вигоди за найменших витрат. Протидія таким методам незаконного отримання інформації визначає напрями дій держави щодо забезпечення власної кібербезпеки. В Україні такі функції покладені найбільшою мірою на спеціальний підрозділ Національної поліції – кіберполіцію. До позитивів її роботи

можна віднести те, що, крім можливостей звернення щодо скоєних злочинів, на сайті кіберполіції функціонує спеціальний сервіс «No more ransom», що пропонує безкоштовний он-лайн сервіс розшифровки даних комп'ютера у випадку атаки з вимогою викупу – доступно з [7].

Разом з тим, стрімкий розвиток IT-ринку, в тому числі його тіньової складової, вимагають посилення уваги не лише до питання покарань за скоєні злочини, але й до методів їх попередження, що більшою мірою визначає кібербезпеку країни та окремих суб'єктів господарювання і населення. Для підтвердження того, що посилення кібербезпеки є не менш важливим напрямом зусиль, порівняно з іншими напрямами національної безпеки, варто проаналізувати наслідки умисних впливів у кіберпростір на різних рівнях економічних відносин.

Статистика за таким видом злочинності поки що відсутня на офіційних інформаційних ресурсах, зокрема, вона не оприлюднюється Державною службою статистики. Тому отримати уявлення про порушення безпеки у кіберпросторі України можна лише на основі запитів до відповідних державних органів. Так, скориставшись даними з відповіді на один з таких запитів, що доступно на сайті «Української правди», можемо констатувати, що поширення тільки офіційно зареєстрованих кіберзлочинів, щодо яких були звернення і які взяті на облік Генеральною прокуратурою України, є дуже суттєвим (рис. 1).

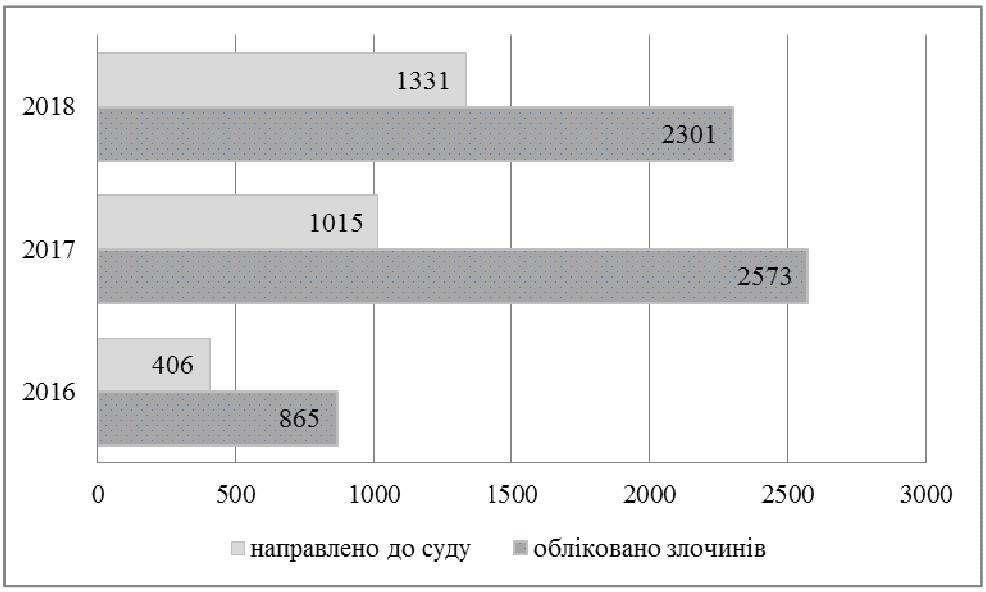

Рис. 1. Динаміка кіберзлочинів, облікованих та направлених до суду Генеральною прокуратурою України у 2016–2018 рр.
(складено авторами за даними [8])

Як бачимо, навіть за статистикою трьох останніх років кількість кіберзлочинів в Україні є дуже невтішною, особливо помітним є її стрімке зростання у 2017 році. При цьому статистика розкриття злочинів суттєво поступається даним щодо їх обліку. Тобто на цьому сегменті суспільних відносин, що фактично є тіньовим ринком ІТ-послуг, можемо констатувати очевидно високий рівень навичок злочинців та слабку поширеність засобів протидії таким злочинів в Україні.

Якщо говорити про їх фінансові наслідки, то таку інформацію взагалі можна отримати лише з окремих досліджень – за згаданим запитом, в якому запитувалась інформація не лише про кількість, але й про фінансові втрати внаслідок злочинів, ГПУ надала лише часткову відповідь, оминувши економічну частину запиту.

Тому можна скористатись наближеними оцінками. Так, за оцінками експертів Kaspersky Lab («Лабораторія Касперського»), що є найбільшим в Європі виробником систем захисту від шкідливого і небажаного програмного забезпечення, хакерських атак і спаму, наша країна є однією з головних «гарячих точок» на кіберкарті світу за рахунок таких загроз. Українські користувачі значною мірою схильні до заражень через неоновлення програмного забезпечення і піратські копії програм. Показово також, що 17% всіх заражень припадає на користувачів, що працюють із застарілою операційною системою Windows XP. Україна займає третю сходинку рейтингу країн з найбільшим ризиком зараження через Інтернет: 35,7% користувачів зіткнулися з веб-загрозами за звітний період. Україна опинилася на 9 сходинці рейтингу країн з найбільшим ризиком зараження мобільними шкідниками (8,39%). Досить високий і ризик зіткнення з локальними загрозами (54,5%). Сюди потрапляють об'єкти, які проникли на комп'ютери шляхом зараження файлів чи знімних носіїв, або спочатку потрапили на комп'ютер не у відкритому вигляді (наприклад, програми в складі складних інсталяторів, зашифровані файли і т.п.) [4, С. 30-31].

Результати ряду досліджень свідчать про низьку ефективність вітчизняних методів боротьби з кіберзлочинністю і недостатню практику їх здійснення, зокрема й шляхом забезпечення вищої обізнаності населення. Так, за даними Української міжбанківської асоціації членів платіжних систем ЕМА, у 2016 році кожен сотий власник платіжної картки в Україні став жертвою шахраїв. Внаслідок вішингу (телефонне шахрайство з виманюванням реквізитів банківських карток і переказом коштів на карту злодіїв) з рахунків українців було вкрадено 275,45 млн грн, а внаслідок фішингу (виманювання конфі-

денційних даних – паролів, номерів банківських карток, PIN-кодів тощо) – 63,68 млн грн, загалом – 339,13 млн грн за 2016 рік. Для порівняння, у 2015 році шахраї викрали з рахунків українців 84,36 млн грн [9]. Як бачимо, стрімкий розвиток IT-технологій та системи електронних переказів є не єдиною передумовою виникнення кібернебезпек – часто негативні економічні наслідки зумовлені відсутністю відповідних знань власників електронних рахунків.

Не маючи даних щодо втрат українських компаній, можемо скористатись досвідом країн, в яких методи боротьби з кіберзагрозами відпрацьовані набагато краще, але й у них, як свідчать дані одного з спеціальних досліджень [10], кіберзлочинність призводить до суттєвих негативних втрат компаній. Для бізнесу найвагомішою такою втратою, через яку виникають й інші види збитків, є втрати часу (рис. 2).

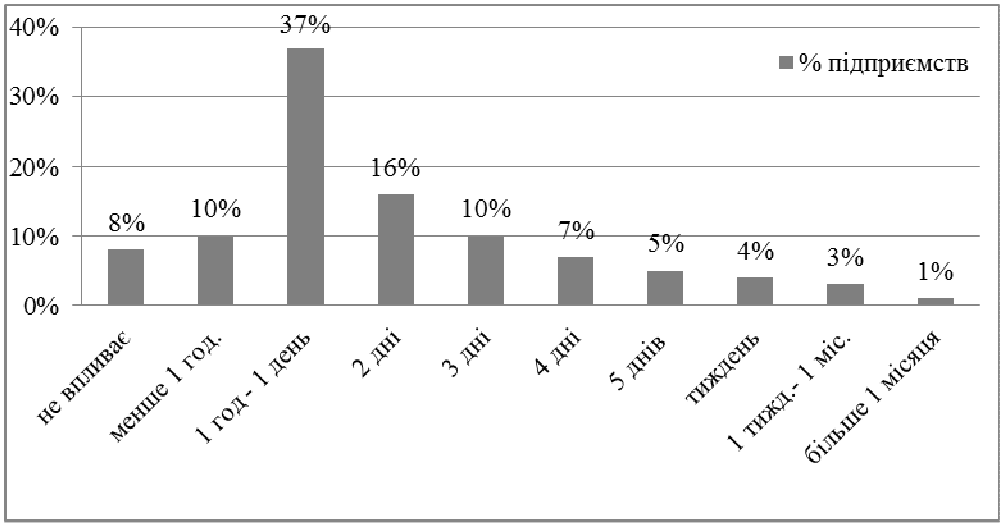

Рис. 2. Час, необхідний для повернення до звичайних умов бізнесу після кібератаки (складено авторами за даними [10, С. 6])

Отже, як бачимо, у більшості випадків нормальна робота інформаційних систем підприємств відновлюється за один день, але є випадки, що вимагають набагато довших зусиль з відновлення нормальної роботи, а отже, і супроводжуються простоями всього підприємства чи його окремих підрозділів та відповідно фінансовими втратами.

При цьому пріоритети у посиленні безпеки інформаційних систем та захисту даних підприємства виглядають наступним чином (табл. 2).

Таблиця 2

Кіберпріоритети на наступні 12 місяців для компаній США, Німеччини та Великобританії (складено автором за даними [10, С. 16])

Пріоритети	Вагомість, на думку:	
	новачків	експертів
Швидка реакція на кіберінциденти	51%	85%
Вирішення існуючих загроз власними силами	48%	82%
Використання хмарних або керованих служб безпеки	42%	80%
Купівля/посилення кіберстрахування	43%	80%

Як бачимо, велика частина підприємств розраховує на виправлення інцидентів власними силами, що, водночас, не заважає оцінювати кіберстрахування як пріоритет. Крім того, як для новачків на ринку, так і на думку експертів, одним з найбільш ефективних методів уникнення кіберзагроз є розвиток хмарних технологій.

Крім цих методів, у розвинених країнах у якості превентивних заходів з посилення кібербезпеки застосовуються також ті, що наведені в табл. 3.

Таблиця 3

Рівень використання додаткових кібер-сервісів компаніями США, Німеччини та Великобританії для попередження кіберризиків, % поширеності у компаніях (складено автором за даними [10, С. 23])

США	
Тренінг працівників	49%
Оцінки ризиків	42%
Профілактичне обладнання/програмне забезпечення	41%
Великобританія	
Тренінг працівників	44%
Найсучасніша інформація про загрози	44%
Оцінки ризиків	41%
Німеччина	
Консультація	44%
Профілактичне обладнання/програмне забезпечення	41%
Тренінг працівників	40%

Як бачимо, дуже велика частка зусиль компаній буде зосереджена не лише на удосконаленні суто технічних параметрів інфор-

маційних систем, зокрема встановленні профілактичного обладнання чи програмного забезпечення. Великого значення власники підприємств надають розвитку навичок персоналу щодо правильного поводження з інформаційними технологіями та ресурсами, а також попередженню негативних наслідків на основі своєчасної оцінки можливих ризиків. Такий досвід разом з іншими кращими практиками у цій сфері корисно застосовувати і в Україні задля посилення кібербезпеки на всіх рівнях.

Висновки. Отже, реаліями економічної діяльності в Україні є істотне зростання кіберзлочинності в останні роки та її суттєві негативні наслідки, що порушують нормальні умови функціонування не лише окремих підприємств та спричиняють дискомфорт та фінансові втрати населення, але й стають одним із ключових сучасних чинників національної фінансово-економічної небезпеки з огляду на стрімке поширення та вагомість впливів: варто тільки згадати одну з атак у вигляді вірусу Petya в кінці червня 2017 року, наслідки якого оцінюють у 0,4% ВВП [11]. Навіть один цей приклад (0,4% річного ВВП за півгодинну атаку) є вагомим аргументом щодо потреби вдосконалення методів поведінки у національному кіберпросторі. Тому за світовим досвідом використання ІТ та поширенням методів попередження кіберзагроз або подолання їх наслідків вважаємо, що найбільш пріоритетними для України мають бути дії щодо посилення обізнаності користувачів щодо кіберзагроз та поведінки у таких ситуаціях, розвиток ринку кіберстрахування, а також посилення державного контролю за національним кіберпростором.

1. World Economic Forum. The Global Risk Reports. URL: https://www.weforum.org/reports (дата звернення: 15.11.2018). **2.** Про основні засади забезпечення кібербезпеки України : Закон України. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.11.2018). **3.** Андрощук Г. О. Кібербезпека: тенденції в світі та Україні. *Кібербезпека та інтелектуальна власність: проблеми правового забезпечення* : матеріали Міжнародної науково-практичної конференції (21 квітня 2017 р., Київ). К. : Вид-во «Політехніка», 2017. С. 30–36. **4.** Колесніков, А., Зяйлик, М. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею. *Актуальні проблеми правознавства.* 2017. № 1. С. 26–29. **5.** Семенуха Р. Як це робила Польща: досвід боротьби з кіберзагрозами. *Економічна правда*. URL: https://www.epravda.com.ua/columns/2017/10/12/630044/ (дата звернення: 15.11.2018). **6.** Конвенція Ради Європи про кіберзлочинність. URL: http://zakon2.rada.gov.ua/laws/show/994_575 (дата звернення: 15.11.2018). **7.** Офіційний сайт Кіберполіції України. URL: https://cyberpolice.gov.ua/ (дата звернення: 15.11.2018). **8.** Кіберзлочинність. Відповідь на запит до Генеральної прокуратури України. *Українська*

правда. URL: https://dostup.pravda.com.ua/request/kibierzlochinnist_6?nocache=incoming-99255#incoming-99255 (дата звернення: 15.11.2018). **9.** Базиленко А. У 2016-му шахраї вкрали з рахунків українців майже 340 млн грн. URL: http://watcher.com.ua/2017/02/07/u-2016-mu-shahrayi-vkraly-z-rahunkiv-ukrayintsiv-mayzhe-340-mln-hrn/ (дата звернення: 15.11.2018). **10.** The Hiscox Cyber Readiness Report 2017. URL: https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017 (дата звернення: 15.11.2018). **11.** Через атаку вірусу Petya Україна за півгодини втратила 10 млрд гривень – експерт. 3.11.2017. Назва з екрану. URL: https://ukr.segodnya.ua/economics/enews/iz-za-ataki-virusa-petya-ukraina-za-polchasa-poteryala-10-mlrd-griven-ekspert-1069181.html (дата звернення: 15.11.2018).

REFERENCES:

1. World Economic Forum. The Global Risk Reports. URL: https://www.weforum.org/reports (data zvernennia: 15.11.2018). **2.** Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (data zvernennia: 15.11.2018). **3.** Androshchuk H. O. Kiberbezpeka: tendentsii v sviti ta Ukraini. Kiberbezpeka ta intelektualna vlasnist: problemy pravovoho zabezpechennia : materialy Mizhnarodnoi naukovo-praktychnoi konferentsii (21 kvitnia 2017 r., Kyiv). K. : Vyd-vo «Politekhnika», 2017. S. 30–36. **4.** Kolesnikov, A., Ziailyk, M. Ekonomiko-pravovi zasady rozvytku kiberzlochynnosti ta metodiv borotby z neiu. Aktualni problemy pravoznavstva. 2017. № 1. S. 26–29. **5.** Semenukha R. Yak tse robyla Polshcha: dosvid borotby z kiberzahrozamy. Ekonomichna pravda. URL: https://www.epravda.com.ua/columns/2017/10/12/630044/ (data zvernennia: 15.11.2018). **6.** Konventsiia Rady Yevropy pro kiberzlochynnist. URL: http://zakon2.rada.gov.ua/laws/show/994_575 (data zvernennia: 15.11.2018). **7.** Ofitsiinyi sait Kiberpolitsii Ukrainy. URL: https://cyberpolice.gov.ua/ (data zvernennia: 15.11.2018). **8.** Kiberzlochynnist. Vidpovid na zapyt do Heneralnoi prokuratury Ukrainy. Ukrainska pravda. URL: https://dostup.pravda.com.ua/request/kibierzlochinnist_6?nocache=incoming-99255#incoming-99255 (data zvernennia: 15.11.2018). **9.** Bazylenko A. U 2016-mu shakhrai vkraly z rakhunkiv ukraintsiv maizhe 340 mln hrn. URL: http://watcher.com.ua/2017/02/07/u-2016-mu-shahrayi-vkraly-z-rahunkiv-ukrayintsiv-mayzhe-340-mln-hrn/ (data zvernennia: 15.11.2018). **10.** The Hiscox Cyber Readiness Report 2017. URL: https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017 (data zvernennia: 15.11.2018). **11.** Cherez ataku virusu Petya Ukraina za pivhodyny vtratyla 10 mlrd hryven – ekspert. 3.11.2017. Nazva z ekranu. URL: https://ukr.segodnya.ua/economics/enews/iz-za-ataki-virusa-petya-ukraina-za-polchasa-poteryala-10-mlrd-griven-ekspert-1069181.html

(data zvernennia: 15.11.2018).

Рецензент: д.е.н., професор Левицька С. О. (НУВГП)

Mishchuk H. Y., Doctor of Economics, Professor (National University of Water and Environmental Engineering, Rivne),
Komar S. O., Senior Student (National University of Water and Environmental Engineering, Rivne)

CYBERCRIME AS AN OUTCOME OF IT-MARKET DEVELOPMENT: ASSESSING CHALLENGES FOR FINANCIAL AND ECONOMIC SECURITY

The dynamics of cybercrimes in Ukraine during 2015-2018 is analyzed. It was established that cybercrime as one of the negative consequences of the IT-market development is a type of crime, without well-developed counteractions in Ukraine. Due to limitations in statistics on its financial and economic implications, foreign experience has been used to characterize enterprise losses and importance among the global risks. The application of the progressive world experience for strengthening cybersecurity in Ukraine is proposed. The main measures which can be useful for financial and economic security of Ukraine as well as for the development of IT-sphere are: actions to increase user awareness of cyber threats and behavior in such situations, the development of the cyber insurance market, and the strengthening of state control of national cyberspace.
***Keywords*: IT-market, cybersecurity, cybercrime, financial and economic consequences.**

Мищук Г. Ю., д.э.н., профессор (Национальный университет водного хозяйства и природопользования, г. Ровно),
Комар С. А., студентка (Национальный университет водного хозяйства и природопользования, г. Ровно)

КИБЕРПРЕСТУПНОСТЬ КАК СЛЕДСТВИЕ РАЗВИТИЯ IT-РЫНКА: ОЦЕНКА ВЫЗОВОВ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Проанализирована динамика киберпреступлений в Украине в течение 2015-2018 годов. Установлено, что киберпреступность как один из негативных последствий развития IT-рынка является тем видом преступлений, противодействие которым пока не имеет дос-

таточного развития в Украине. Имея ограничения в статистических данных для анализа последствий для финансово-экономической безопасности Украины, использован зарубежный опыт для характеристики потерь предприятий, а также значимости в числе глобальных рисков человечества. Предложено применение прогрессивного мирового опыта для усиления кибербезопасности в Украине. Основными являются действия по усилению осведомленности пользователей о киберугрозах и поведении в таких ситуациях, развитие рынка киберстрахования, а также усиление государственного контроля национального киберпространства.
***Ключевые слова*: IT-рынок, кибербезопасность, киберпреступность, финансово-экономические последствия.**
